Section 12: Verification of Identity and Authority

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the identity and authority verification of the person requesting PHI and the documentation required to substantiate the PHI disclosure request.

Policy

Identification of person requesting PHI

The IHCP must verify the identity of the person requesting PHI, and whether the person has the authority to access PHI, if the identity or such authority of the person is not known to the IHCP. Also, the IHCP must obtain any documentation, statements, or representations (written or oral) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure. The IHCP Privacy Office will be responsible for those disclosures requiring verification and documentation.

Member Requests for Access to PHI

Some member requests for access to PHI will be forwarded to the IHCP Privacy Office for response. The IHCP Privacy Office will handle all written requests.

However, some requests from members will be handled directly by FSSA/OMPP staff members.

Staff members must follow required protocols prior to releasing any PHI to members. See Appendix G for protocols.

Verification

The IHCP will continue to verify the identity of a member who is requesting the use or disclosure of his or her own PHI.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, any prior disclosure made at the member's request are not required to be documented in this accounting.

Note: Please refer to Section 11 of this manual, *IHCP Member Access to Protected Health Information,* for specific details.

Member's Personal Representative Requesting PHI Access

Some member personal representative requests for access to PHI will be forwarded to the IHCP Privacy Office for response. The IHCP Privacy Office will handle all written requests.

However, some requests will be handled directly by FSSA/OMPP staff members.

Staff members must follow required protocols prior to releasing any PHI to a member or their personal representative. See Appendix G for protocols, and Appendix I for the *Personal Representative Authorization Form.*

Verification

A member's personal representative or legal guardian must provide documentation verifying their authority to request the member's PHI, and must be authorized to act as the member's personal representative. See Appendix I for the *Personal Representative Authorization Form.*

For PHI requests initiated by a member's personal representative, the *Verification of Identity and Authority* form will be used to verify identity (see Appendix C). FSSA/OMPP staff members should refer the requestor to the IHCP Privacy Office to obtain this form for their completion.

Accounting of disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, any prior disclosure made pursuant to the member personal representative's request is not required to be documented in this accounting.

Note: Please refer to Section 11 of this manual, *IHCP Member Access to Protected Health Information,* for specific details.

All Other External Entities Requesting PHI Disclosure

The IHCP may disclose a member's PHI to an external entity with the appropriate authorization from the member or the member's personal representative.

In most cases, the member will request PHI disclosure from the IHCP to an external entity, such as a legislator or attorney.

Documentation Requirements

The IHCP will require that the member, or the member's personal representative, submit a written, valid authorization prior to releasing the PHI to an external entity, except under the circumstances described in Section 10 "Permitted disclosure of PHI without written authorization".

All authorizations must meet the criteria for a proper and valid written authorization.

All authorizations for the disclosure of PHI received from members or member personal representatives will be forwarded to the IHCP Privacy Office for response.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, this accounting is not required to include any disclosure made pursuant to the member's, or the member personal representative's authorization.

Note: Please refer to Section 14 of this manual, *Member Authorization to Release Protected Health Information,* for specific details.

When member authorization is not required

The IHCP may use or disclose a member's PHI to an external entity, without the member's (or member's personal representative) authorization under specific circumstances. There are some situations in

which the IHCP is required to notify the member of the PHI use or disclosure, and some in which the member can agree to the use or disclosure. In these situations, the IHCP may provide notification verbally to the member and the member can give agreement verbally.

(Refer to Section 10 "Permitted disclosure of PHI without written authorization" for specific information).

Verification of authority

The IHCP must verify the identity of the person requesting PHI and the authority of the person to have access to PHI, if the identity or such authority of the person is not known to the IHCP.

Documentation Requirements

Also, the IHCP must obtain any documentation, statements, or representations (written) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure.

If the PHI disclosure is conditioned on particular documentation, statements, or representations (written) from the person requesting the PHI, the IHCP may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that meet the requirements.

An administrative subpoena or similar process or by a separate written statement that demonstrates the applicable requirements have been met will satisfy the requirement for a disclosure for law enforcement purposes, if:

- The information requested is relevant and material to a legitimate law enforcement inquiry;
- The request is specific and limited in scope to a reasonable extent for the purpose; and
- De-identified information could not be reasonably used.

Verification of requests made by public officials

The IHCP may rely, if reasonable under the circumstances, on any of the following to verify identity when the PHI disclosure is to a public official or a person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested or an oral statement of the legal authority, if the written statement is not practical; or
- A warrant, subpoena, order, or other legal process issued by a grand

Verification of requests made by public officials (continued)

jury or a judicial or administrative tribunal if a request is made pursuant to a legal process; or

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; or
- If the request is in writing, the written request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of the public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order), that establishes that the person is acting on behalf of the public official.
- If the public official is a legislator, authorization from the member is needed. Written requests may include a signed and authorized HIPAA compliant form or an Authorization to Act on Behalf of Constituent Form, or written correspondence or e-mail received from the constituent which includes verifiable personal information (such as social security number, case number and/or date of birth) and which clearly authorizes a Legislative (see Appendix H) staff member to receive the confidential information. In the absence of a written request, personal knowledge of the constituent's agreement to the release of the confidential information through participation in a meeting or conference call, which includes the constituent and a member of the agency's legislative team, may be sufficient.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, these uses and disclosures will be documented on the *Accounting of Disclosures* as requested by the member, except for those cases involving:

- National security and intelligence activities; or
- Correctional institutions and other law enforcement custodial situations.

Note: Please refer to the *Uses and Disclosures of Protected Health Information When Member Authorization is not Required* Section 10 and the *Accounting of Disclosures to Member* Section 18, for specific details.

Procedure

Requests for PHI

The IHCP Privacy Office will manage all requests for copies of PHI. This includes requests for copies of PHI that may be maintained by FSSA/OMPP staff.

NOTE: Authorized staff members may continue to use and disclose PHI within the authorized, routine duties of their assigned positions. In these situations, staff members will be responsible for verification of the requestor's identification and authority prior to releasing PHI. Appropriate procedures to follow when carrying out these authorized duties are detailed throughout the appropriate sections of this manual, and in Appendix G.

Example of FSSA/OMPP staff responsibility

Member John Doe calls the staff member to ask a question regarding his PHI. Staff member Y should first verify the identity of John Doe, according to outlined procedures in this section and in *Appendix G* of this manual. Once identity is verified, staff member Y may respond to John Doe's request.

If a copy of a member's PHI is requested, the requestor should be referred to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.514(h)

Section 13: Member Request for Amendment of Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to member amendment to PHI.

Policy

Member Rights

A member has the right to request an amendment to the member's PHI or a record about the member in the designated record set from the IHCP for as long as the PHI is maintained by the IHCP. Notice of these rights and the process for the member to follow to exercise them are provided to each IHCP member in the *Notice of Privacy Practices*.

Requirements for PHI Amendment Requests

The IHCP requires that the member, or the member's personal representative, make a written request using the *Member Amendment Request* form (see Appendix D).

The IHCP will require that the request contain a statement providing a reason for the amendment, the records to be amended, and whom the member wants the IHCP to notify regarding the amendment.

Response to Amendment Requests

All requests for amendments should be referred to the IHCP Privacy Office. The Privacy Office will provide the requestor with the appropriate form, and will document, review, and respond to the requesting member within the timeframes required by the *Privacy Rule,* after receipt of the written request. The IHCP may deny a request as appropriate.

When the IHCP is not the originator of the PHI

In most instances when PHI is requested, the IHCP is not the originator of the information. In this case, the IHCP will refer the member to the healthcare provider originating the PHI. This should result in minimal amendments to PHI within IHCP.

Procedure

The IHCP Privacy Office will manage all requests from members related to the amendment of their PHI.

If a member requests that their PHI be corrected refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.526

Section 14: Member Authorization to Release Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members' authorization to release PHI.

Policy

When Member Authorization is required to use, disclose, or request PHI

The IHCP must have proper and written authorization from the member, or the member's personal representative, before the IHCP can use, disclose to, or request PHI from, another covered entity for **any purpose EXCEPT** for:

- Treatment;
- Payment;
- Health care operations; or
- As permitted or required by law without authorization (See *Uses and Disclosures of Protected Health Information When Member Authorization is Not Required*, Section 10 for additional detail).

A member's authorization is required for the use or disclosure of psychotherapy notes, with exceptions.

Use and disclosure of authorized PHI

When the IHCP obtains or receives a member's valid authorization for the IHCP's use or disclosure of PHI, the use and disclosure must be consistent with the authorization.

IHCP initiates the request for authorization

There may be rare cases in which the IHCP initiates a request for authorization from the member to release their PHI to an external entity. If the IHCP requests a member's authorization to disclose PHI to an external entity, the IHCP must return copy of the member's signed authorization form to them.

Member initiates the request for authorization

When the member requests the release of PHI to an external entity, such as a legislator or attorney, the IHCP will require that the member, or the member's personal representative, submit a written, valid authorization.

All authorizations will be documented, reviewed, and addressed by the IHCP Privacy Office. There are no set timeframes required by the *Privacy Rule* for this procedure.

Accounting of disclosures

If a member, or a member's personal representative, requests an accounting of disclosures of their PHI made by the IHCP, any disclosure made pursuant to an authorization is not required to be documented in this accounting.

Revocation of authorization

The member can, at any time, revoke all or part of their authorization by giving written notice of the revocation to the IHCP Privacy Office.

The *Right to Revoke* notice is documented in the *Notice of Privacy Practices* document and also within the *Member Authorization* form (see Appendix E).

The IHCP will require that the member submit the revocation in writing, using the *Revocation of Authorization* form.

(See Appendix E).

Procedure

Requests to release PHI

The IHCP Privacy Office will manage all requests from members related to the release of their PHI to third parties, e.g. relatives, personal representatives, member of the Legislature, etc.

If a member requests that their PHI be released to a third party refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Revocation of authorization

The Privacy Office will manage all requests for revocation of authorization.

The member must submit the request to revoke authorization to the IHCP Privacy Office, in writing, as described in the *Notice of Privacy Practices* document mailed to all IHCP members. The IHCP Privacy Office, or external unit (i.e., OMPP, EDS general, HCE or ACS) will forward the *Revocation of Authorization* form to the member for completion upon request from the member. If a member submits a request for an authorization revocation, the IHCP Privacy Office will forward the *Revocation of Authorization* form to the member for completion.

The *Revocation of Authorization* form will be received in the IHCP Privacy Office, stamped with the receipt date, and logged into the Member Authorization Tracking System. If the request is received into another unit within the OMPP, EDS, or HCE, the external unit will forward the request to the IHCP Privacy Office.

The IHCP Privacy Office staff member will review the member's authorization revocation request and document the information in the Member Authorization Tracking System.

A copy of the *Revocation of Authorization Receipt* letter will be sent to the member. One copy of the response will be maintained in the Privacy Office.

> *Note: A member may revoke the authorization, in writing, at any time except to the extent that the IHCP has already taken action in reliance on the authorization.*

The authorization revocation request and response(s), including all correspondence, will be retained for six (6) years from the later of the date of creation or the date when the authorization revocation was last in effect in the IHCP Privacy Office.

Regulatory Requirements and Authority: 45 CFR 164.508

Section 15: Member Request for Alternate Communication

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to members' rights relating to alternate communication requirements for PHI.

Policy

Member Rights

A member has the right to make a request to the IHCP requesting that the IHCP communicate their PHI to them in a certain way or at a certain location. Notices of these rights and the process for members to follow are provided to each IHCP member in the *Notice of Privacy Practices* document.

How to request alternate communication

The IHCP will require that the member, or the member's personal representative, make a written request using the *Alternate Communication Request* form (see Appendix F).

All requests for alternate communication of PHI will be documented, reviewed, and responded to the requesting member within the timeframes required by the HIPAA *Privacy Rule*.

Requirements of the IHCP in approval or denial of requests

The IHCP must accommodate reasonable requests for communicating with a member by alternate means at alternate locations, if the member clearly states that the disclosure of all or part of the PHI could endanger the member.

The IHCP may approve or deny alternate communication requests and is not required to agree to a confidential communication request unless the member indicates endangerment.

If the IHCP agrees to communicate with the member through alternate means, it must communicate as agreed upon with the member in order not to violate the agreement.

Procedure

Right to request alternate communication

Members have a right to request that their information, such as the NPP or copies of their PHI, be sent to them in an alternative manner or to an alternative location, relative to the standard method of providing this information to them.

Examples of alternate communication

This may take the form of requesting electronic copies instead of paper or that the information be mailed to an address other than the address on the eligibility file.

Requests for alternate communication

Any requests from members for alternate communication should be referred to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.522(b)

Section 16: Member Complaints

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members' complaints about alleged violations of their rights relating to PHI.

As a covered entity under HIPAA, the IHCP must provide a process for a member to make complaints concerning its privacy policies and procedures, as well as its compliance with these policies and procedures. This policy and procedure document sets forth that process for the IHCP.

Policy

Member Rights

A member of IHCP has the right to file a complaint to the IHCP and to the Secretary if they believe that their privacy rights have been violated.

In addition, the member has the right to file a complaint with the Secretary of HHS if they believe that the IHCP is not complying with the applicable requirements of the *Privacy Rule*.

Notice of these rights and the process for the member to follow to exercise them are provided to each IHCP member in the *Notice of Privacy Practices*.

Filing a Complaint

The IHCP will suggest the member to file the complaint with the IHCP Privacy Office in writing and within 180 days of the incident for which the complaint is being registered.

Requirements of the IHCP

All complaints received will be documented and investigated, and a response provided to the complainant, with a copy provided to the OMPP Privacy Coordinator.

The IHCP will not take any retaliatory action against a member who has filed a complaint with the IHCP or with the Secretary of HHS.

Procedure

Member complaints regarding use of their PHI

The IHCP Privacy Office will be responsible for receiving, reviewing, and responding to complaints from members regarding use of their PHI.

If a member complains that the IHCP has misused their PHI please refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority:
45 CFR 164.520(b)(1)(vi)
45 CFR 164.530(d)(1)

Section 17: Member Request to Restrict Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members request to restrict uses and disclosures of PHI.

Policy

Member Rights

A member has the right to request that the IHCP to restrict the uses and disclosures of his or her PHI as it relates to treatment, payment, or health care operations and other disclosures permitted by the *Privacy Rule*.

Notices of these rights and the process for the member to follow are provided to each IHCP member in the *Notice of Privacy Practices* document.

How to request a restriction on use of PHI

The IHCP will require that the member, or the member's personal representative, make a written request for a restriction and to specify the type of information to be included in the restriction, to whom the restriction applies, and the effective dates of the restriction period.

See Appendix J to access the *Member Restriction Request Form*.

IHCP Authority

The OMPP Privacy Coordinator has the authority to approve or deny restriction requests. The IHCP is not required to agree to a restriction; however, if the IHCP agrees to a restriction, it may not use or disclose the PHI to the restricted parties without violating the restriction.

Required exclusions to restricted use

A restriction agreed to by the IHCP does not prevent the uses or disclosures of PHI that are permitted or required as follows:

- When required by the Secretary to investigate or determine the IHCP's compliance with the *Privacy Rule*;
- For public health activities if required by law;
- To other government agencies providing benefits or services to the individual;
- To government agencies that oversee health care programs;
- For research (if related to a State Plan purpose); and
- For other uses and disclosures that are required by law.

Refer to the *Uses and Disclosures of Protected Health Information When Member Authorization is Not Required*, Section 10, for specific activities permitted or required by law for the IHCP to use or disclose PHI.

Termination of Restriction

The IHCP may terminate its agreement to a restriction, if:

- The member agrees to or requests the termination in writing;
- The member orally agrees to the termination and the oral agreement is documented; or
- The IHCP informs the member that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the member.

Procedure

Requests for restricted use of PHI

The IHCP Privacy Office will manage all requests from members to restrict the use of their PHI.

If a member requests that the use of their PHI be restricted refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority:
45 CFR 164.522(a)
45 CFR 164.502(c)

Section 18: Accounting of Disclosures to Member

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the accounting for disclosures, to IHCP members, of their PHI.

Policy

Requirements of the IHCP

The IHCP must account to an IHCP member, or a member's personal representative, for PHI disclosures, as required by the *Privacy Rule* for those instances in which the PHI is released to an external entity for purposes other than treatment, payment, or health care operations.

When an accounting of disclosures is not required by the IHCP

The majority of PHI received and disclosed by the IHCP is used for treatment, payment, and operations, so the disclosure of PHI for other purposes should be minimal. The IHCP **is not required** to account for disclosures:

- To carry out treatment, payment and health care operations;
- To IHCP members (for PHI about them);
- To a member's personal representative;
- To correctional institutions or law enforcement officials; or
- That occurred prior to the compliance date (April 14, 2003).

When an accounting of disclosures is required by the IHCP

The IHCP **will be required** to account for disclosures, such as those:

- For research;
- To other government agencies providing benefits or service to members, or that oversee health care providers (if the disclosure does not meet the definition of treatment, payment, or health care operations); or

- Any other disclosure that is not identified as being excluded above.

Documentation Requirements

Disclosures that require an accounting must be documented so that an accounting can be provided to the member if requested. All requests for accounting of disclosures will be documented, reviewed, and responded to within the timeframes required by the *Privacy Rule*. Refer to Appendix K for the *Member Accounting Request Form*.

Availability of historical disclosures

The disclosure of a member's PHI must be accounted for six years and will commence April 14, 2003.

The member can request a six-year history, but this cannot be created for disclosures prior to the April implementation date.

Cost per disclosure accounting

The IHCP will provide one free disclosure accounting per member each 12 months. The IHCP may charge the member for each additional disclosure accounting during the same 12-month period.

Additional Information

IHCP Privacy Office staff members will follow the policies and procedures contained in their manual to comply with the *Privacy Rule* for uses and disclosures of PHI.

See the *Permitted and Required Uses and Disclosures of Protected Health Information*, Section 3, for additional information.

Procedure

Required Documentation

Any PHI that is released to any person or entity, other than the member, for purposes other then treatment, payment, or healthcare operations (TPO) must be documented and an accounting provided to the member, if requested by the member, for up to six years, beginning April 14, 2003.

See the *Glossary* section of this manual for a detailed description of TPO.

Release of PHI

FSSA/OMPP staff members **are not** authorized to release any PHI for purposes other than TPO, unless they have been approved to do so, and such release has been coordinated with the OMPP Privacy Coordinator.

Requests for Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI, they must complete a *Member Accounting Request Form* (provided in Appendix K of this manual), and submit the completed form to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Charging the Member for Accounting of Disclosure Copies and Mailings

If the accounting of disclosures request from the member or member's personal representative meets the criteria for charging, the member or personal representative must be notified in writing of the charge prior to the accounting copying and mailing. The *Disclosure Accounting* letter will be mailed to the member to provide the copying and mailing charges that would result from the accounting request.

The member is instructed to contact the IHCP Privacy Office to make arrangements. A personal check or money order will be accepted as payment. All payments received into the IHCP Privacy Office will be tracked and be forwarded to the EDS Finance Unit for deposit.

Suspended Rights

The IHCP must temporarily suspend a member's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such an agency or official, if the agency or official provides the IHCP with a written statement that such an accounting to the member would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

Regulatory Requirements and Authority: 45 CFR 164.528

Section 19: Safeguards for Staff use of Protected Health Information Access

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to workforce members access to, and use of, IHCP members' PHI.

Policy

Requirements of the IHCP: Access Limitations

The *Privacy Rule* requires that safeguards be in place to limit unnecessary or inappropriate access to protected health information. To be in compliance, the IHCP must apply the minimum necessary requirements, including access and use by the FSSA/OMPP staff and contractor staff, for most PHI uses and disclosures.

The IHCP shall limit access and use of PHI by its staff and contractors to the minimum necessary to accomplish the defined work functions.

The requirements also apply to PHI requests made by, or on behalf of, the IHCP to another covered entity.

The access limitations apply to all paper, fax, oral, and electronic communication of PHI. This is inclusive of Indiana*AIM* along with any other database or repository of information containing PHI.

Exclusions to access limitation requirements

There are instances in which the minimum necessary limitation is not required, including:

- Disclosures made to a member's health care provider for the purpose of providing treatment;
- Disclosures made to the member or through the member's written authorization in regard to their own PHI; or
- Uses or disclosures required by law, including the HIPAA *Privacy Rule*.

Refer to Section 4 of this manual, *Minimum Necessary Requirements*, for additional information.

Procedure

Paper Communication

All paper communication that contains PHI, to any entity outside of the IHCP, must be contained within a sealed envelope or other protective cover to prevent the inadvertent disclosure of PHI to an unauthorized person. This includes courier service to EDS or HCE, mail to IHCP providers or members, PHI forwarded to other IHCP contractors, or any other entity that has been authorized to receive the PHI.

Hard copy documents containing PHI must be protected as described in the *Protected Health Information Safeguards* section of this manual. FSSA/OMPP staff members who are not required to use PHI in their work functions are prohibited from PHI access, unless prior approval has been received from their direct supervisor.

Fax Communication

All fax communication containing PHI, provided to any entity outside of the IHCP, must be accompanied by a cover sheet containing the statement:

"This facsimile transmission (and attachments) may contain protected health information from the IHCP, which is intended only for the use of the individual or entity named in this transmission sheet. Any unintended recipient is hereby notified that the information is privileged and confidential, and any use, disclosure, or reproduction of this information is prohibited. Any unintended recipient should contact Jenifer Nelson, OMPP Privacy Coordinator, by telephone at (317) 233-0446 immediately."

Fax documents containing PHI must be protected as described in the *Protected Health Information Safeguards* section of this manual. FSSA/OMPP staff members who are not required to use PHI in their work functions are prohibited from PHI access, unless prior approval has been received from their direct supervisor.

Oral Communication

All oral communication concerning a member's PHI must be limited to the nature of the intended work and will only be discussed in the appropriate area within the IHCP. No PHI communication of any type is to be discussed outside of the IHCP workspace, including other areas within the building complex.

E-Mail Communication

PHI communicated via e-mail text or attachments, to any FSSA/OMPP staff member or external entity, should always be limited to the minimum necessary amount of information that is needed exclusively to carry out treatment, payment, or operations (TPO). E-mail transmissions of PHI must only be made to individuals who are authorized to receive such information, and files containing PHI that are exchanged with outside entities (i.e., outside of the secure State network) should be encrypted with the "Certified Mail" tool, or the currently approved OMPP encryption tool. In addition, the following statement will be systematically generated at the bottom of all email messages:

"The information contained in this E-mail and/or attachments may contain protected health, legally privileged, or otherwise confidential information intended only for the use of the individual(s) named above. If you, the reader of this message, are not the intended recipient, you are hereby notified that you may not further disseminate, distribute, disclose, copy or forward this message or any of the content herein. If you have received this E-mail in error, please notify the sender immediately and delete the original."

All questions concerning e-mail transmission of PHI are to be referred to the OMPP Privacy Coordinator for resolution.

Indiana*AIM* Access

On a periodic basis, all IHCP management staff will review the quarterly Indiana*AIM* class summary for their business unit, in relation to PHI access via Indiana*AIM,* in order to answer the following questions:

- Are the Indiana*AIM* profiles for the workforce classes in their respective units, specifically those that provide access to member PHI, still necessary for staff to perform their work functions?
- Are the actual Indiana*AIM* access classes currently assigned to the staff members in their units the same in comparison to the pre-assigned profiles for the workforce class for each staff member?
- Are all staff members assigned to the unit classes currently working in the unit?
- Are any staff members who currently work in the unit, but are not listed on the quarterly profile for the business unit, assigned to another unit's access class?

Modification to Indiana*AIM* classes

For any change needed to modify the Indiana*AIM* access profiles for the work unit, the IHCP manager will notify the OMPP Privacy Coordinator of the needed change. No action is necessary if no changes are recommended.

For any staff member found to be on the unit access profile who is not currently working in the unit, notify the OMPP Privacy Coordinator of the need to delete all Indiana*AIM* access for that staff member. Also notify the staff member's current manager of the access deletion and the need to request the appropriate Indiana*AIM* access for the new job function.

For any staff member who is not found to be on the unit access profile, forward the appropriate Indiana*AIM* access profile request for the staff member to the EDS Security Unit.

Regulatory Requirements and Authority:
45 CFR 164.514(d)(2)(i)
45 CFR 164.530(c)(1)

Section 20: Protected Health Information Safeguards

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the:

- administrative,
- technical, and
- physical safeguards

to adequately protect IHCP members' PHI.

Policy

Responsibility of FSSA/OMPP Staff

It is the responsibility of all FSSA/OMPP staff and contractor staff to reasonably protect all members PHI from inappropriate use or disclosure.

OMPP is housed in a secure self-contained area. OMPP workforce members are authorized to enter this area through one of three doors, which require a four-digit access code for entrance. Each individual OMPP staff member has a unique access code that permits entrance into the facility. The access code is not to be shared with anyone else.

Visitor controls are in place to limit outside entrance into facilities. Visitors may enter the OMPP facility through one door, which is monitored during all operating hours by a receptionist. There is a waiting area with available seats for guests; seats are positioned away from areas where PHI could be visible. Visitors must be approved for entrance, sign a log of visitation, wear a visitation badge and be escorted by an authorized OMPP staff member at all times.

Types of Member PHI Requiring Safeguards

All IHCP members PHI in written, electronic, or oral form is protected by the *Privacy Rule* and must be safeguarded in the work place and in the daily job functions of all FSSA/OMPP staff members.

This includes PHI access through the IHCP office or through off-site access.

Unauthorized use or disclosure of PHI by FSSA/OMPP staff	Any unauthorized use or disclosure by an FSSA/OMPP staff member will be subject to the sanctions set forth by the IHCP for breach of security or privacy. Refer to Section 21, *Sanctions,* for additional details.

Procedure

FSSA/OMPP Staff Responsibilities	All FSSA/OMPP staff are responsible to help ensure that the appropriate administrative safeguards are followed to protect against the unauthorized use of a member's PHI. All OMPP staff are also responsible for assisting in controlling and validating a person's access to facilities.
Work Station Requirements	FSSA/OMPP staff are to maintain a secure personal working environment that: • Safeguards PHI while they are not at their station; • Maintains the positioning of their computer screen to ensure that PHI is protected from unauthorized viewing; • Implements password protection controls as required by DTS; • Removes records containing PHI from desktops and places such records in locked drawers or file cabinets; • Ensures that all drawers containing PHI are closed and locked; • Ensures that PHI is not left unattended in the aisles; and • Does not allow unauthorized visitors into the IHCP work area.
Disposal of documents containing PHI	FSSA/OMPP staff must ensure that paper documents containing PHI are shredded prior to their disposal.

Regulatory Requirements and Authority:
45 CFR 164.514(d)(2)(ii)
45 CFR 164.530(c)(1-2)

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to sanctions against workforce members who fail to comply with the established privacy policies and procedures.

Policy

Sanctions against IHCP workforce members

The IHCP is required to develop, and apply when appropriate, sanctions against members of its workforce who fail to comply with privacy policies or procedures or with the requirements of the *Privacy Rule.*

Types of Sanctions

The IHCP is required to develop and impose sanctions appropriate to the nature of the violation.

The type of sanction may vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of PHI.

Sanctions could range from a warning to termination.

These sanctions do not apply to whistleblower activities.

Documentation Requirements

The IHCP is required to have written policies and procedures for the application of appropriate sanctions for violations of the *Privacy Rule* and to document those sanctions.

Documentation must be retained for six years by the Privacy Coordinator.

Procedure

FSSA/OMPP staff violation of the *Privacy Rule*

FSSA/OMPP staff who violate the privacy requirement of HIPAA are subject to appropriate sanctions which may include suspension or termination.

Sanctions will be imposed in accordance with FSSA guidelines.

Mitigation

Pursuant to 45 CFR 164.30(f), the IHCP must mitigate, to the extent practicable, any harmful effect that is known from any use or disclosure of PHI, by a staff member or a business associate of the IHCP, in violation of IHCP policies and procedures, or the requirements of the *Privacy Rule*.

Regulatory Requirements and Authority: 45 CFR 164.530(e)

Purpose

To provide instructions for the IHCP in regard to the training of all FSSA/OMPP staff in regard to HIPAA privacy regulations.

Policy

The OMPP Privacy Coordinator will ensure that all FSSA/OMPP staff receive training, and periodic re-training, on HIPAA policies and procedures as necessary and appropriate for their function with IHCP.

Procedure

Training and certification of FSSA/OMPP Staff	The OMPP Privacy Coordinator is responsible for ensuring that all FSSA/OMPP staff are trained concerning privacy requirements.
Documentation	The OMPP Privacy Coordinator will maintain all records to document this training.
Existing FSSA/OMPP Staff	The OMPP Privacy Coordinator will ensure that all existing FSSA/OMPP staff receive privacy training and obtain a passing score on the post-training evaluation.
New FSSA/OMPP Staff	The OMPP Privacy Coordinator will ensure that all new FSSA/OMPP staff are provided with the privacy training module and obtain a passing score on the post-training evaluation.
Re-training Requirements	On a periodic basis, the OMPP Privacy Coordinator will arrange for IHCP-wide privacy re-training.

Regulatory Requirements and Authority: 45 CFR 164.530(b)